МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«Национальный исследовательский ядерный университет «МИФИ»»

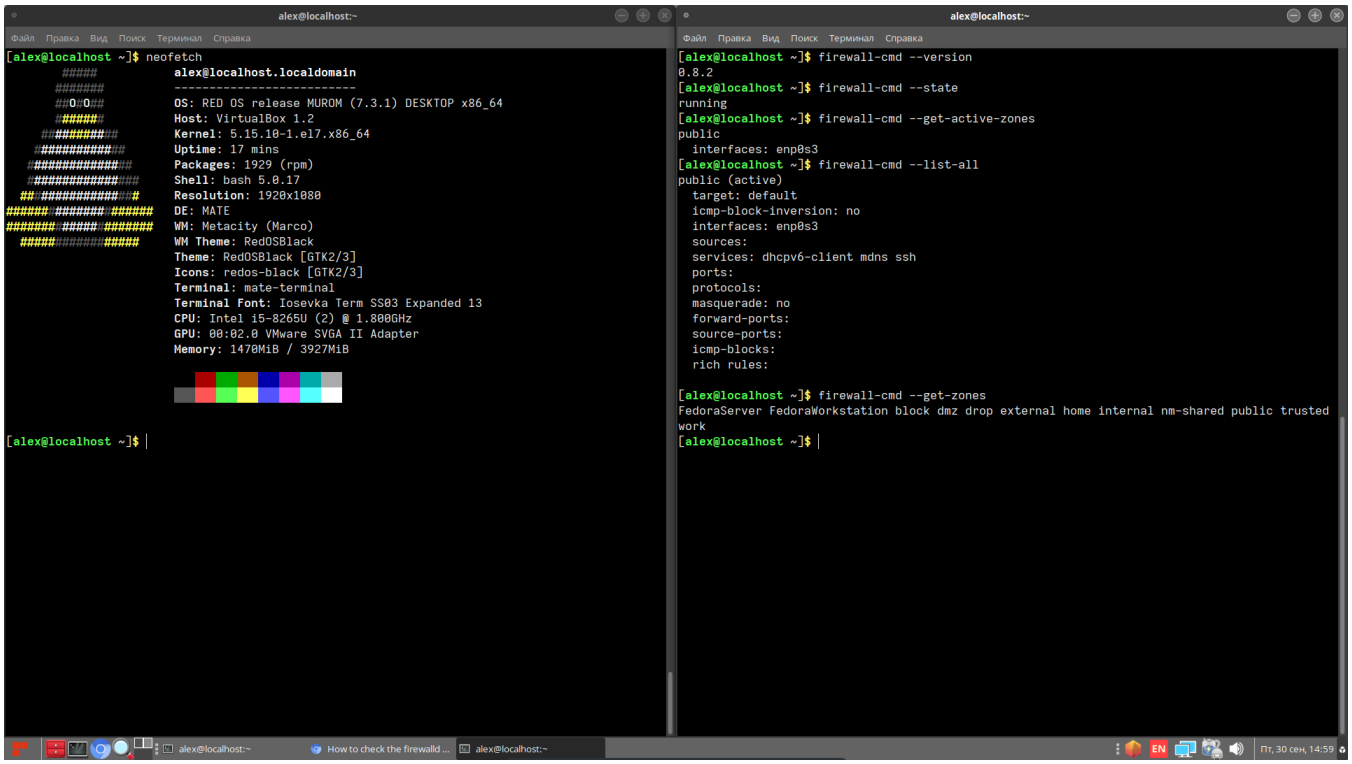
ЛАБОРАТОРНАЯ РАБОТА №2:
«Настройка персональных межсетевых экранов»

Выполнили студенты группы Б19-515
Щербакова Александра
Белов Александр

Москва, 2022 г.

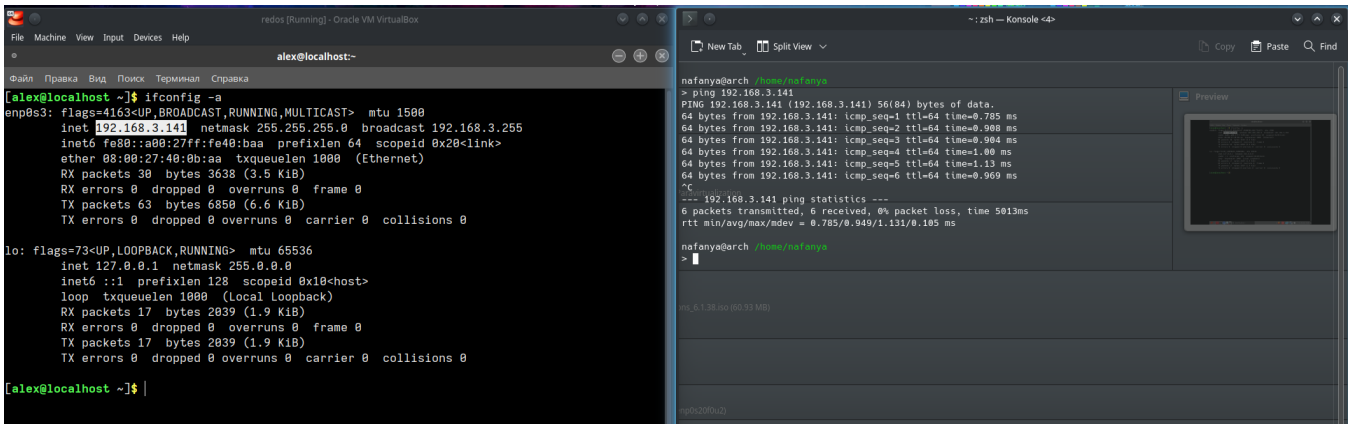
Часть 1. Работа с зонами firewalld

1. Образ RedOS Муром скачан, виртуальная машина создана, firewalld установлен.



Работа с зоной public

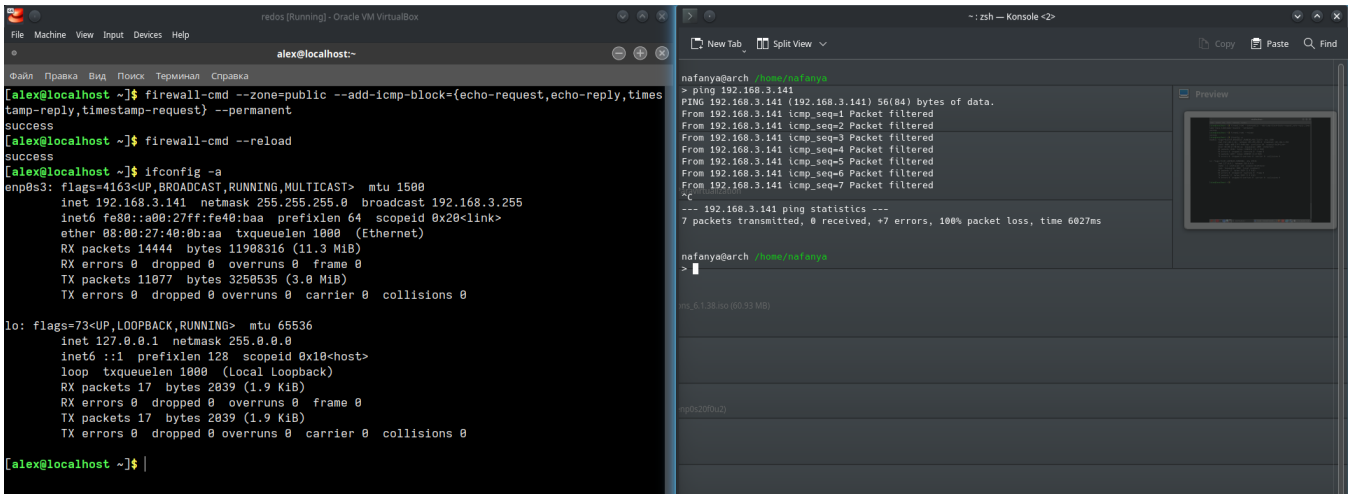
1. Запретить icmp. Скриншот до применения запрещающего правила (слева - консоль виртуальной машины, справа - консоль хоста)



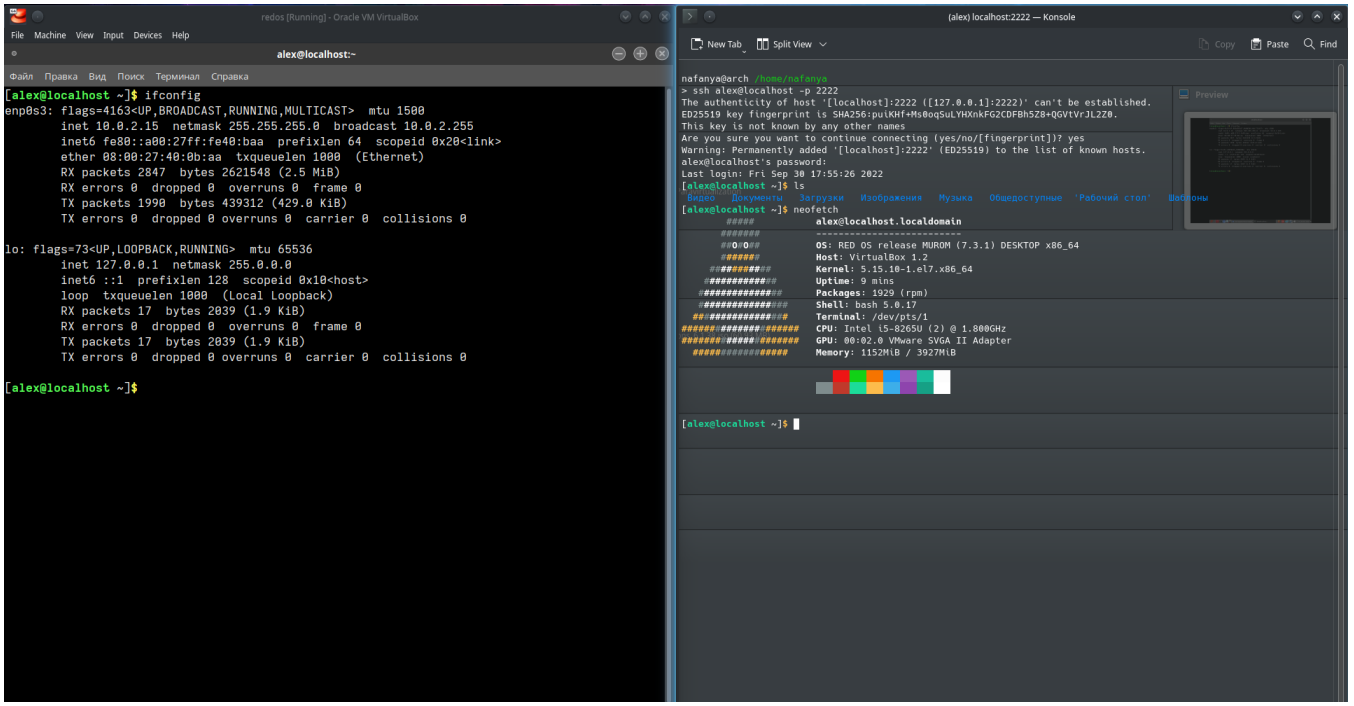
После применения запрещающего правила, а именно

```
[alex@localhost ~]$ firewall-cmd --zone=public --add-icmp-block={echo-request,echo-reply,timestamp-reply,timestamp-request} --permanent
```

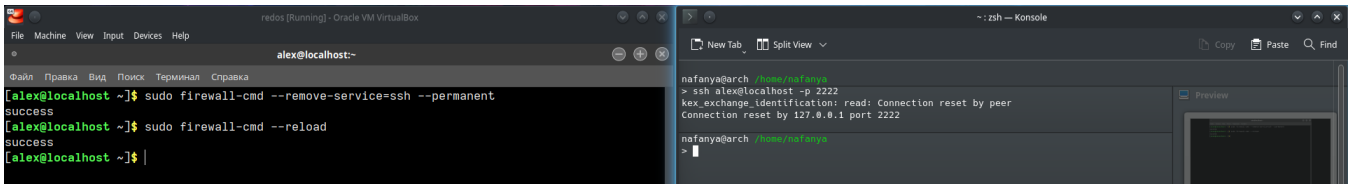
пингануть виртуальную машину не получается



2. Запретить ssh. Изначально к виртуальной машине можно подключиться по ssh:



После применения блокирующего правила подключиться к виртуальной машине по ssh нельзя:



Работа с зоной drop

1. Установить в качестве сетевой зоны drop:

```
[alex@localhost ~]$ sudo firewall-cmd --get-active-zones
public
  interfaces: enp0s3
[alex@localhost ~]$ sudo firewall-cmd --zone=drop --change-interface=
enp0s3  lo
[alex@localhost ~]$ sudo firewall-cmd --zone=drop --change-interface=enp0s3
success
[alex@localhost ~]$ sudo firewall-cmd --get-active-zones
drop
  interfaces: enp0s3
```

2. Попытаться подключиться по ssh:

```
nafanya@arch /home/nafanya
> ssh alex@localhost -p 2222
kex_exchange_identification: read: Connection reset by peer
Connection reset by 127.0.0.1 port 2222
```

Подключиться нельзя, так как зона drop сбрасывает весь входящий трафик без ответа. Согласно документации:
drop: самый низкий уровень доверия сети. Весь входящий трафик сбрасывается без ответа, поддерживаются только исходящие соединения.
public: эта зона представляет публичную сеть, которой нельзя доверять, однако поддерживает входящие соединения в индивидуальном порядке.

Часть 2. Работа с iptables

1. Запретить входящий трафик по протоколу tcp:

```
[alex@localhost ~]$ sudo iptables --list
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
[alex@localhost ~]$ sudo iptables -A INPUT -p tcp -j DROP
[alex@localhost ~]$ sudo iptables --list
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       tcp  --  anywhere             anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

2. Разрешить входящий трафик по протоколу tcp:

```
[alex@localhost ~]$ sudo iptables --flush
[alex@localhost ~]$ sudo iptables --list
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
[alex@localhost ~]$ sudo iptables -A INPUT -p tcp -j ACCEPT
[alex@localhost ~]$ sudo iptables --list
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  anywhere             anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

3. Запретить входящий трафик по порту 22:

```
[alex@localhost ~]$ sudo iptables --flush
[alex@localhost ~]$ sudo iptables -A INPUT -p tcp --dport 22 -j DROP
[alex@localhost ~]$ sudo iptables --list
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       tcp  --  anywhere             anywhere             tcp dpt:ssh

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

4. Разрешить входящий трафик по порту 22:

```
[alex@localhost ~]$ sudo iptables --flush
[alex@localhost ~]$ sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPT
[alex@localhost ~]$ sudo iptables --list
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:ssh

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

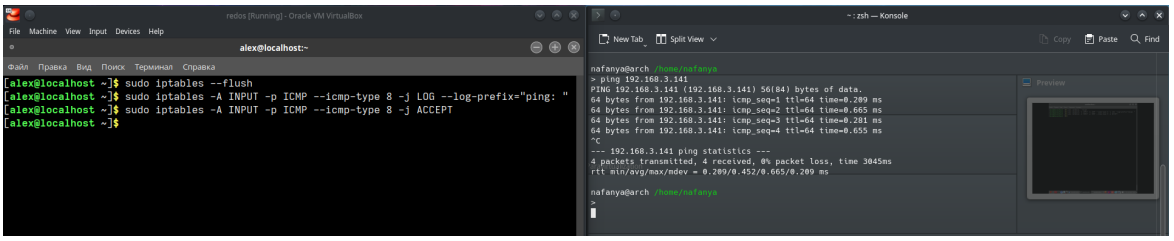
5. Запретить исходящий трафик по порту 443:

```
[alex@localhost ~]$ sudo iptables --flush
[alex@localhost ~]$ sudo iptables -A OUTPUT -p tcp --dport 443 -j DROP
[alex@localhost ~]$ sudo iptables --list
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
DROP       tcp  --  anywhere             anywhere             tcp dpt:https
[alex@localhost ~]$
```

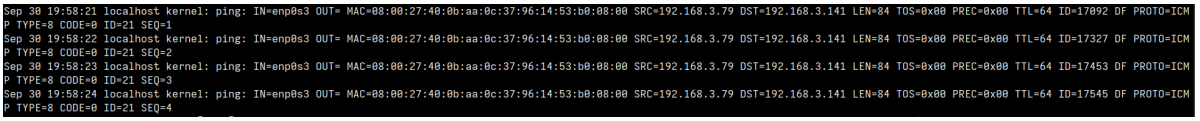
6. Разрешить исходящий трафик по порту 443:

```
[alex@localhost ~]$ sudo iptables --flush
[alex@localhost ~]$ sudo iptables -A OUTPUT -p tcp --dport 443 -j ACCEPT
[alex@localhost ~]$ sudo iptables --list
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:https
[alex@localhost ~]$
```

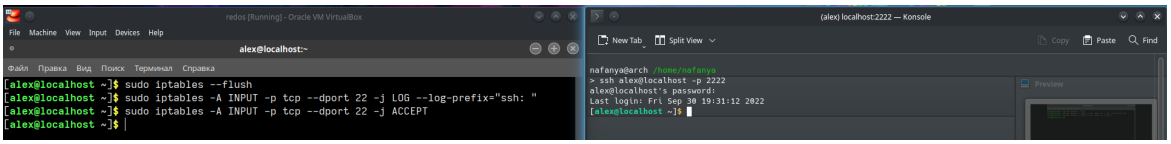
7. Написать правила для журналирования
   a. Всех icmp-пакетов



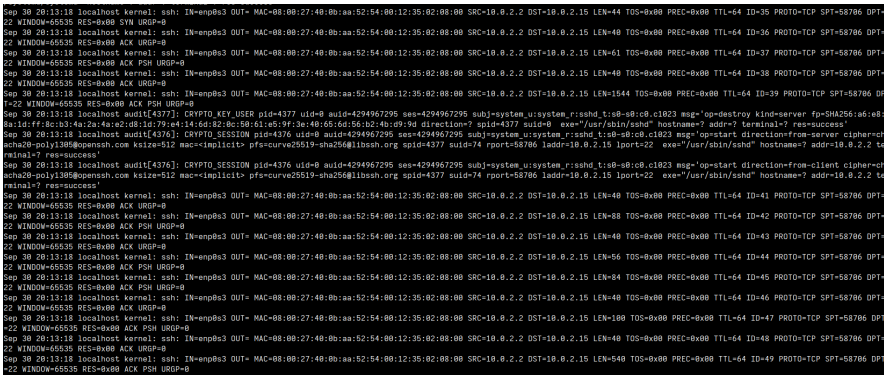
После этого в файле /var/log/messages виртуальной машины появятся строки

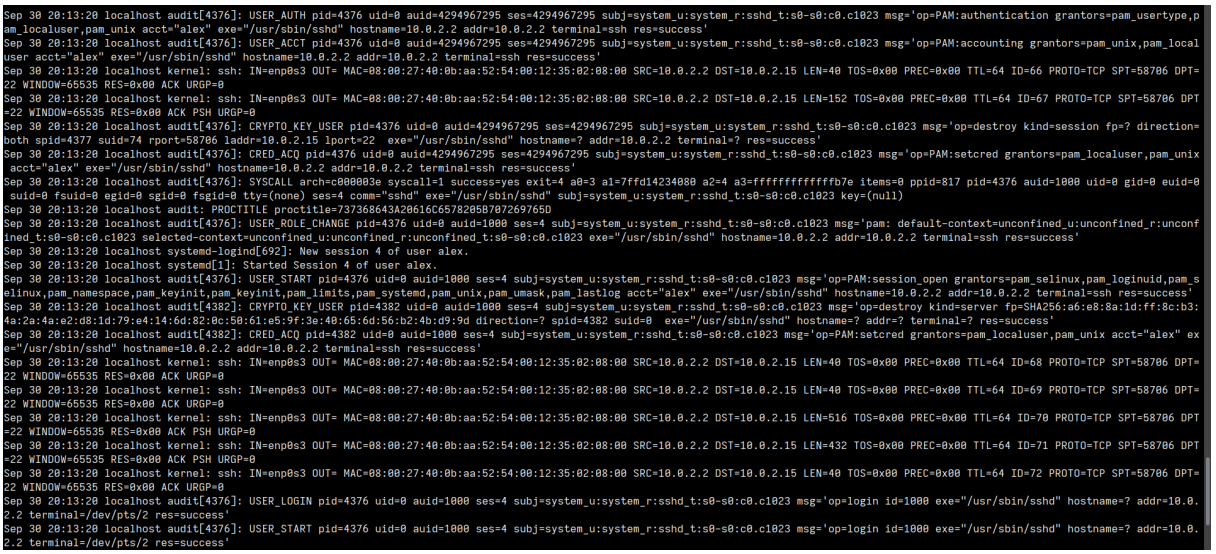


   b. Пакетов, приходящих на 22 порт



После этого в файле /var/log/messages виртуальной машины появятся строки


Sep 30 20:13:18 localhost kernel: ssh: IN=enp0s3 OUT= MAC=08:00:27:40:0b:aa:52:54:00:12:35:02:08:00 SRC=10.0.2.2 DST=10.0.2.15 LEN=44 TOS=0x00 PREC=0x00 TTL=64 ID=35 PROTO=TCP SPT=58706 DPT=22 WINDOW=65535 RES=0x00 SYN URGP=0
Sep 30 20:13:18 localhost kernel: ssh: IN=enp0s3 OUT= MAC=08:00:27:40:0b:aa:52:54:00:12:35:02:08:00 SRC=10.0.2.2 DST=10.0.2.15 LEN=40 TOS=0x00 PREC=0x00 TTL=64 ID=36 PROTO=TCP SPT=58706 DPT=22 WINDOW=65535 RES=0x00 ACK URGP=0
Sep 30 20:13:18 localhost kernel: ssh: IN=enp0s3 OUT= MAC=08:00:27:40:0b:aa:52:54:00:12:35:02:08:00 SRC=10.0.2.2 DST=10.0.2.15 LEN=61 TOS=0x00 PREC=0x00 TTL=64 ID=37 PROTO=TCP SPT=58706 DPT=22 WINDOW=65535 RES=0x00 ACK PSH URGP=0
Sep 30 20:13:18 localhost kernel: ssh: IN=enp0s3 OUT= MAC=08:00:27:40:0b:aa:52:54:00:12:35:02:08:00 SRC=10.0.2.2 DST=10.0.2.15 LEN=40 TOS=0x00 PREC=0x00 TTL=64 ID=38 PROTO=TCP SPT=58706 DPT=22 WINDOW=65535 RES=0x00 ACK URGP=0
Sep 30 20:13:18 localhost kernel: ssh: IN=enp0s3 OUT= MAC=08:00:27:40:0b:aa:52:54:00:12:35:02:08:00 SRC=10.0.2.2 DST=10.0.2.15 LEN=1544 TOS=0x00 PREC=0x00 TTL=64 ID=39 PROTO=TCP SPT=58706 DPT=22 WINDOW=65535 RES=0x00 ACK PSH URGP=0
Sep 30 20:13:18 localhost audit[4377]: CRYPTO_KEY_USER pid=4377 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:sshd_t:s0-s0:c0.c1023 msg='op=destroy kind=server fp=SHA256:a6:e8:8a:1d:ff:8c:b3:4a:2a:4a:e2:d8:1d:79:e4:14:6d:82:0c:50:61:e5:9f:3e:40:65:6d:56:b2:4b:d9:9d direction=? spid=4377 suid=0 exe="/usr/sbin/sshd" hostname=? addr=? terminal=? res=success'
Sep 30 20:13:18 localhost audit[4376]: CRYPTO_SESSION pid=4376 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:sshd_t:s0-s0:c0.c1023 msg='op=start direction=from-server cipher=chacha20-poly1305@openssh.com ksize=512 mac=<implicit> pfs=curve25519-sha256@libssh.org spid=4377 suid=74 rport=58706 laddr=10.0.2.15 lport=22 exe="/usr/sbin/sshd" hostname=? addr=10.0.2.2 terminal=? res=success'
Sep 30 20:13:18 localhost audit[4376]: CRYPTO_SESSION pid=4376 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:sshd_t:s0-s0:c0.c1023 msg='op=start direction=from-client cipher=chacha20-poly1305@openssh.com ksize=512 mac=<implicit> pfs=curve25519-sha256@libssh.org spid=4377 suid=74 rport=58706 laddr=10.0.2.15 lport=22 exe="/usr/sbin/sshd" hostname=? addr=10.0.2.2 terminal=? res=success'
Sep 30 20:13:18 localhost kernel: ssh: IN=enp0s3 OUT= MAC=08:00:27:40:0b:aa:52:54:00:12:35:02:08:00 SRC=10.0.2.2 DST=10.0.2.15 LEN=40 TOS=0x00 PREC=0x00 TTL=64 ID=41 PROTO=TCP SPT=58706 DPT=22 WINDOW=65535 RES=0x00 ACK URGP=0
Sep 30 20:13:18 localhost kernel: ssh: IN=enp0s3 OUT= MAC=08:00:27:40:0b:aa:52:54:00:12:35:02:08:00 SRC=10.0.2.2 DST=10.0.2.15 LEN=88 TOS=0x00 PREC=0x00 TTL=64 ID=42 PROTO=TCP SPT=58706 DPT=22 WINDOW=65535 RES=0x00 ACK PSH URGP=0
Sep 30 20:13:18 localhost kernel: ssh: IN=enp0s3 OUT= MAC=08:00:27:40:0b:aa:52:54:00:12:35:02:08:00 SRC=10.0.2.2 DST=10.0.2.15 LEN=40 TOS=0x00 PREC=0x00 TTL=64 ID=43 PROTO=TCP SPT=58706 DPT=22 WINDOW=65535 RES=0x00 ACK URGP=0
Sep 30 20:13:18 localhost kernel: ssh: IN=enp0s3 OUT= MAC=08:00:27:40:0b:aa:52:54:00:12:35:02:08:00 SRC=10.0.2.2 DST=10.0.2.15 LEN=56 TOS=0x00 PREC=0x00 TTL=64 ID=44 PROTO=TCP SPT=58706 DPT=22 WINDOW=65535 RES=0x00 ACK PSH URGP=0
Sep 30 20:13:18 localhost kernel: ssh: IN=enp0s3 OUT= MAC=08:00:27:40:0b:aa:52:54:00:12:35:02:08:00 SRC=10.0.2.2 DST=10.0.2.15 LEN=84 TOS=0x00 PREC=0x00 TTL=64 ID=45 PROTO=TCP SPT=58706 DPT=22 WINDOW=65535 RES=0x00 ACK PSH URGP=0
Sep 30 20:13:18 localhost kernel: ssh: IN=enp0s3 OUT= MAC=08:00:27:40:0b:aa:52:54:00:12:35:02:08:00 SRC=10.0.2.2 DST=10.0.2.15 LEN=40 TOS=0x00 PREC=0x00 TTL=64 ID=46 PROTO=TCP SPT=58706 DPT=22 WINDOW=65535 RES=0x00 ACK URGP=0
Sep 30 20:13:18 localhost kernel: ssh: IN=enp0s3 OUT= MAC=08:00:27:40:0b:aa:52:54:00:12:35:02:08:00 SRC=10.0.2.2 DST=10.0.2.15 LEN=100 TOS=0x00 PREC=0x00 TTL=64 ID=47 PROTO=TCP SPT=58706 DPT=22 WINDOW=65535 RES=0x00 ACK PSH URGP=0
Sep 30 20:13:18 localhost kernel: ssh: IN=enp0s3 OUT= MAC=08:00:27:40:0b:aa:52:54:00:12:35:02:08:00 SRC=10.0.2.2 DST=10.0.2.15 LEN=40 TOS=0x00 PREC=0x00 TTL=64 ID=48 PROTO=TCP SPT=58706 DPT=22 WINDOW=65535 RES=0x00 ACK URGP=0
Sep 30 20:13:18 localhost kernel: ssh: IN=enp0s3 OUT= MAC=08:00:27:40:0b:aa:52:54:00:12:35:02:08:00 SRC=10.0.2.2 DST=10.0.2.15 LEN=540 TOS=0x00 PREC=0x00 TTL=64 ID=49 PROTO=TCP SPT=58706 DPT=22 WINDOW=65535 RES=0x00 ACK PSH URGP=0

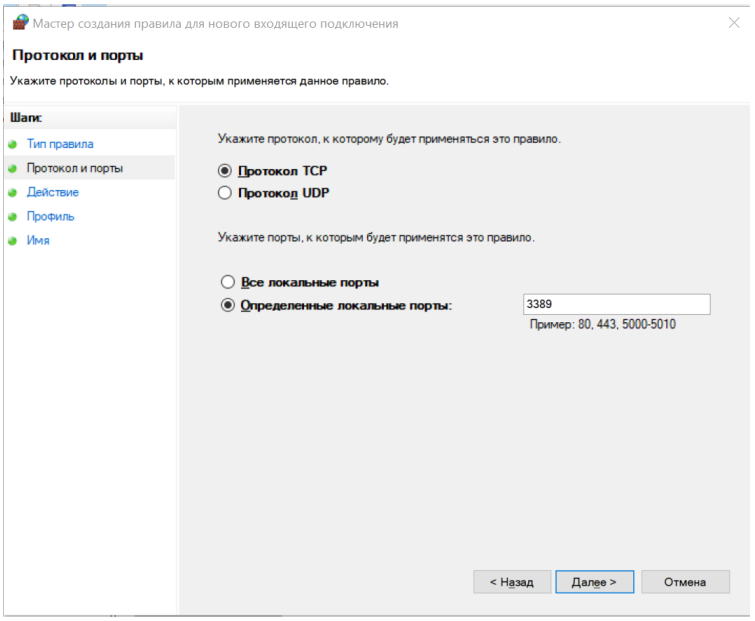

Sep 30 20:13:20 localhost audit[4376]: USER_AUTH pid=4376 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:sshd_t:s0-s0:c0.c1023 msg='op=PAM:authentication grantors=pam_usertype,pam_localuser,pam_unix acct="alex" exe="/usr/sbin/sshd" hostname=10.0.2.2 addr=10.0.2.2 terminal=ssh res=success'
Sep 30 20:13:20 localhost audit[4376]: USER_ACCT pid=4376 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:sshd_t:s0-s0:c0.c1023 msg='op=PAM:accounting grantors=pam_unix,pam_localuser acct="alex" exe="/usr/sbin/sshd" hostname=10.0.2.2 addr=10.0.2.2 terminal=ssh res=success'
Sep 30 20:13:20 localhost kernel: ssh: IN=enp0s3 OUT= MAC=08:00:27:40:0b:aa:52:54:00:12:35:02:08:00 SRC=10.0.2.2 DST=10.0.2.15 LEN=40 TOS=0x00 PREC=0x00 TTL=64 ID=66 PROTO=TCP SPT=58706 DPT=22 WINDOW=65535 RES=0x00 ACK URGP=0
Sep 30 20:13:20 localhost kernel: ssh: IN=enp0s3 OUT= MAC=08:00:27:40:0b:aa:52:54:00:12:35:02:08:00 SRC=10.0.2.2 DST=10.0.2.15 LEN=152 TOS=0x00 PREC=0x00 TTL=64 ID=67 PROTO=TCP SPT=58706 DPT=22 WINDOW=65535 RES=0x00 ACK PSH URGP=0
Sep 30 20:13:20 localhost audit[4376]: CRYPTO_KEY_USER pid=4376 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:sshd_t:s0-s0:c0.c1023 msg='op=destroy kind=session fp=? direction=both spid=4377 suid=74 rport=58706 laddr=10.0.2.15 lport=22 exe="/usr/sbin/sshd" hostname=? addr=10.0.2.2 terminal=? res=success'
Sep 30 20:13:20 localhost audit[4376]: CRED_ACQ pid=4376 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:sshd_t:s0-s0:c0.c1023 msg='op=PAM:setcred grantors=pam_localuser,pam_unix acct="alex" exe="/usr/sbin/sshd" hostname=10.0.2.2 addr=10.0.2.2 terminal=ssh res=success'
Sep 30 20:13:20 localhost audit[4376]: SYSCALL arch=c000003e syscall=1 success=yes exit=4 a0=3 a1=7ffd14234080 a2=4 a3=ffffffffffffffb7e items=0 ppid=817 pid=4376 auid=1000 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none) ses=4 comm="sshd" exe="/usr/sbin/sshd" subj=system_u:system_r:sshd_t:s0-s0:c0.c1023 key=(null)
Sep 30 20:13:20 localhost audit: PROCTITLE proctitle=737368643A20616C6578205B707269765D
Sep 30 20:13:20 localhost audit[4376]: USER_ROLE_CHANGE pid=4376 uid=0 auid=1000 ses=4 subj=system_u:system_r:sshd_t:s0-s0:c0.c1023 msg='pam: default-context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 selected-context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 exe="/usr/sbin/sshd" hostname=10.0.2.2 addr=10.0.2.2 terminal=ssh res=success'
Sep 30 20:13:20 localhost systemd-logind[692]: New session 4 of user alex.
Sep 30 20:13:20 localhost systemd[1]: Started Session 4 of user alex.
Sep 30 20:13:20 localhost audit[4376]: USER_START pid=4376 uid=0 auid=1000 ses=4 subj=system_u:system_r:sshd_t:s0-s0:c0.c1023 msg='op=PAM:session_open grantors=pam_selinux,pam_loginuid,pam_selinux,pam_namespace,pam_keyinit,pam_keyinit,pam_limits,pam_systemd,pam_unix,pam_umask,pam_lastlog acct="alex" exe="/usr/sbin/sshd" hostname=10.0.2.2 addr=10.0.2.2 terminal=ssh res=success'
Sep 30 20:13:20 localhost audit[4382]: CRYPTO_KEY_USER pid=4382 uid=0 auid=1000 ses=4 subj=system_u:system_r:sshd_t:s0-s0:c0.c1023 msg='op=destroy kind=server fp=SHA256:a6:e8:8a:1d:ff:8c:b3:4a:2a:4a:e2:d8:1d:79:e4:14:6d:82:0c:50:61:e5:9f:3e:40:65:6d:56:b2:4b:d9:9d direction=? spid=4382 suid=0 exe="/usr/sbin/sshd" hostname=? addr=? terminal=? res=success'
Sep 30 20:13:20 localhost audit[4382]: CRED_ACQ pid=4382 uid=0 auid=1000 ses=4 subj=system_u:system_r:sshd_t:s0-s0:c0.c1023 msg='op=PAM:setcred grantors=pam_localuser,pam_unix acct="alex" exe="/usr/sbin/sshd" hostname=10.0.2.2 addr=10.0.2.2 terminal=ssh res=success'
Sep 30 20:13:20 localhost kernel: ssh: IN=enp0s3 OUT= MAC=08:00:27:40:0b:aa:52:54:00:12:35:02:08:00 SRC=10.0.2.2 DST=10.0.2.15 LEN=40 TOS=0x00 PREC=0x00 TTL=64 ID=68 PROTO=TCP SPT=58706 DPT=22 WINDOW=65535 RES=0x00 ACK URGP=0
Sep 30 20:13:20 localhost kernel: ssh: IN=enp0s3 OUT= MAC=08:00:27:40:0b:aa:52:54:00:12:35:02:08:00 SRC=10.0.2.2 DST=10.0.2.15 LEN=40 TOS=0x00 PREC=0x00 TTL=64 ID=69 PROTO=TCP SPT=58706 DPT=22 WINDOW=65535 RES=0x00 ACK URGP=0
Sep 30 20:13:20 localhost kernel: ssh: IN=enp0s3 OUT= MAC=08:00:27:40:0b:aa:52:54:00:12:35:02:08:00 SRC=10.0.2.2 DST=10.0.2.15 LEN=516 TOS=0x00 PREC=0x00 TTL=64 ID=70 PROTO=TCP SPT=58706 DPT=22 WINDOW=65535 RES=0x00 ACK PSH URGP=0
Sep 30 20:13:20 localhost kernel: ssh: IN=enp0s3 OUT= MAC=08:00:27:40:0b:aa:52:54:00:12:35:02:08:00 SRC=10.0.2.2 DST=10.0.2.15 LEN=432 TOS=0x00 PREC=0x00 TTL=64 ID=71 PROTO=TCP SPT=58706 DPT=22 WINDOW=65535 RES=0x00 ACK PSH URGP=0
Sep 30 20:13:20 localhost kernel: ssh: IN=enp0s3 OUT= MAC=08:00:27:40:0b:aa:52:54:00:12:35:02:08:00 SRC=10.0.2.2 DST=10.0.2.15 LEN=40 TOS=0x00 PREC=0x00 TTL=64 ID=72 PROTO=TCP SPT=58706 DPT=22 WINDOW=65535 RES=0x00 ACK URGP=0
Sep 30 20:13:20 localhost audit[4376]: USER_LOGIN pid=4376 uid=0 auid=1000 ses=4 subj=system_u:system_r:sshd_t:s0-s0:c0.c1023 msg='op=login id=1000 exe="/usr/sbin/sshd" hostname=? addr=10.0.2.2 terminal=/dev/pts/2 res=success'
Sep 30 20:13:20 localhost audit[4376]: USER_START pid=4376 uid=0 auid=1000 ses=4 subj=system_u:system_r:sshd_t:s0-s0:c0.c1023 msg='op=login id=1000 exe="/usr/sbin/sshd" hostname=? addr=10.0.2.2 terminal=/dev/pts/2 res=success'

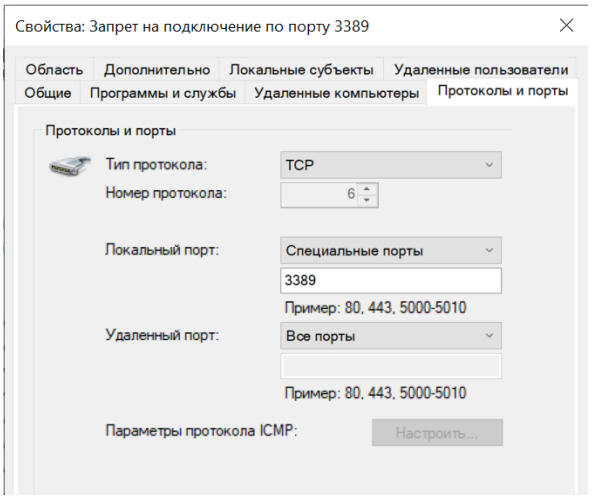
Часть 3. Работа с Windows Firewall

В настройках брандмауэра Windows созданы следующие правила для входящего трафика:

1. *Запрет на подключение по порту 3389*
   Брандмауэр Защитника Windows - Дополнительные параметры - Правила для входящих подключений - Создать правило

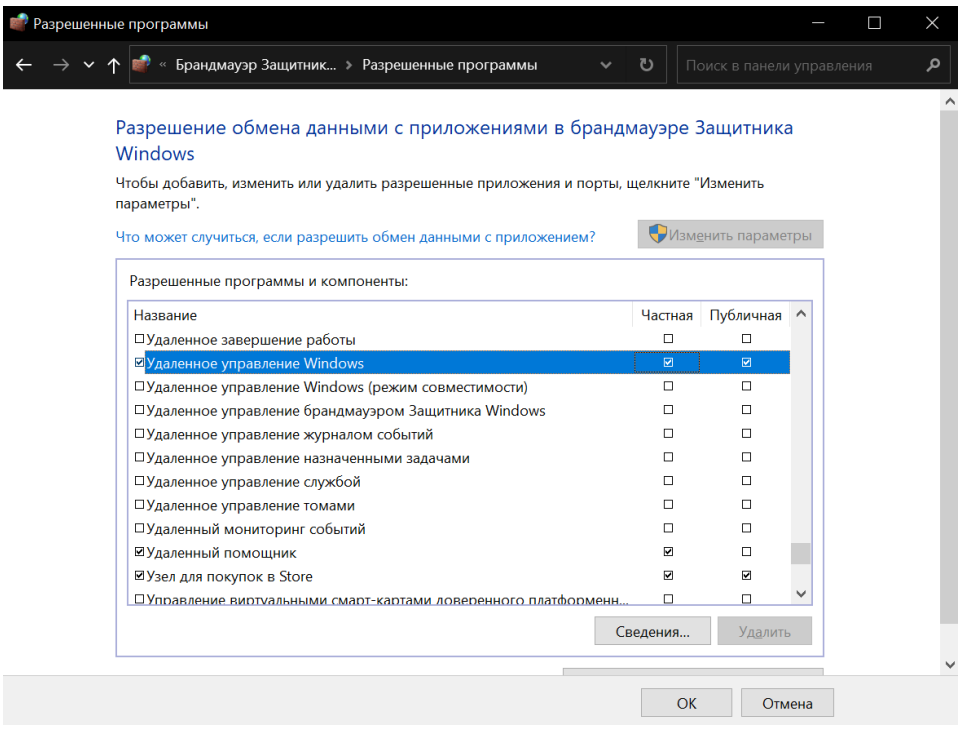
   Тип правила: Для порта;
   Протокол: TCP;
   Определенный локальный порт: 3389;
   Действие: Блокировать подключение.



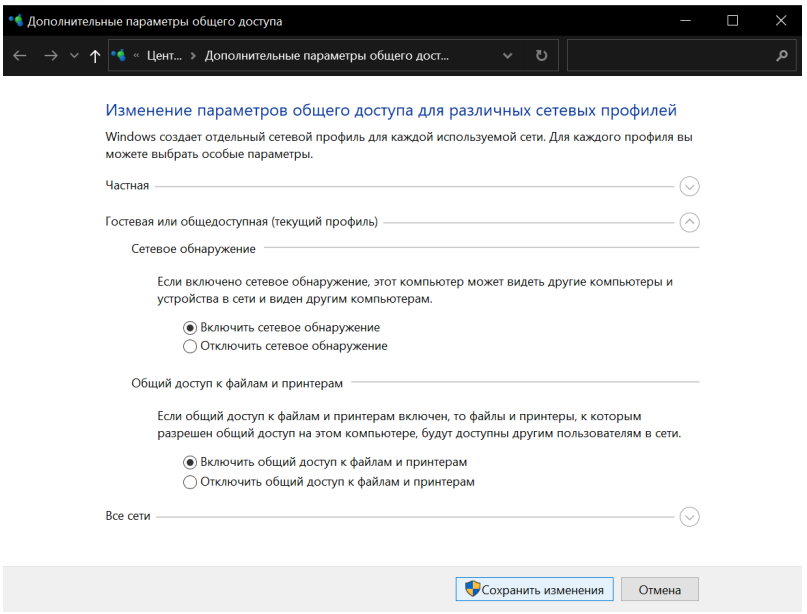


Порт 3389 в ОС Windows 10 используется по умолчанию для удаленного подключения.

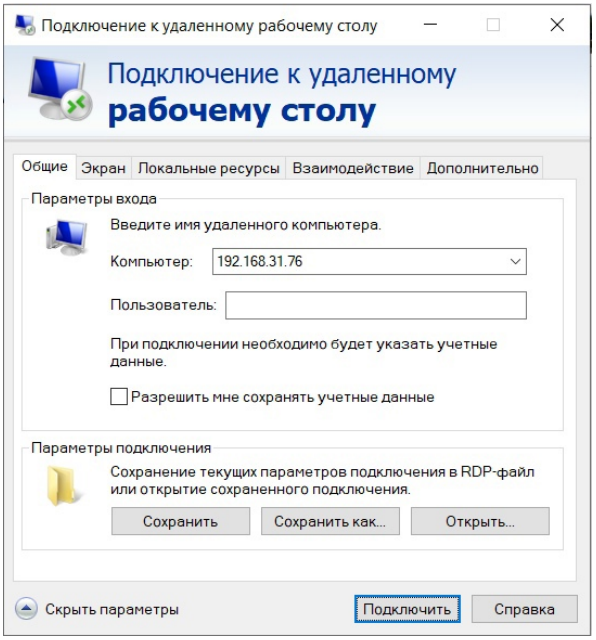
Для проверки работы созданного правила осуществлена попытка подключиться удаленно к рабочему столу. В настройках брандмауэра разрешено удаленное управление Windows, в настройках системы включен удаленный рабочий стол.

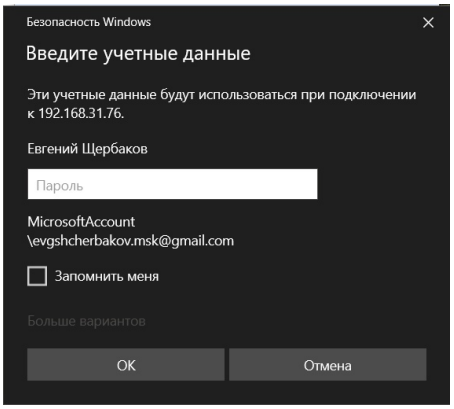


В расширенных настройках общего доступа включено сетевое обнаружение и общий доступ к файлам и принтерам.

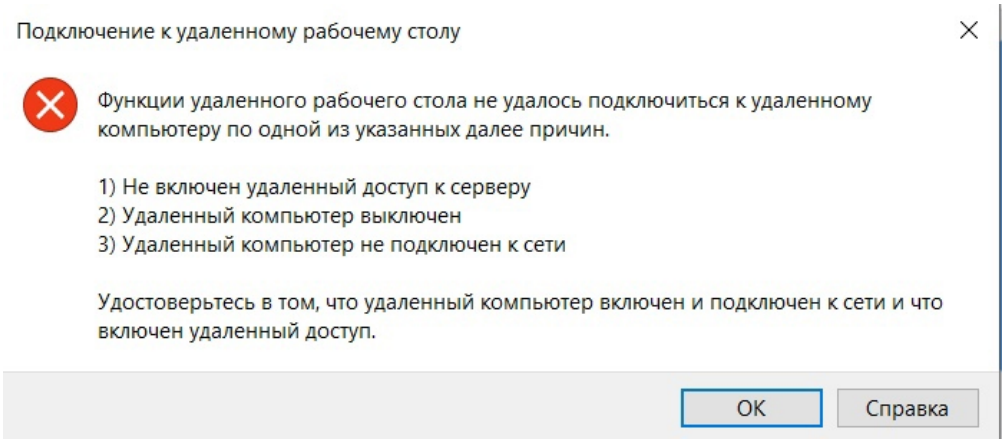


Со второго компьютера инициирован запрос на удаленный доступ. При открытом порте 3389 запрос сработал:



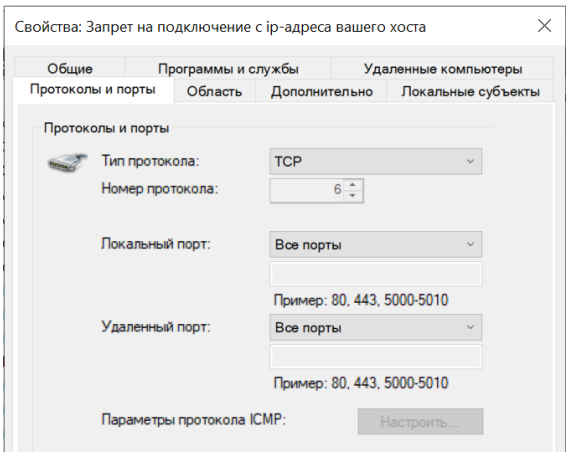


При закрытом порте ошибка:



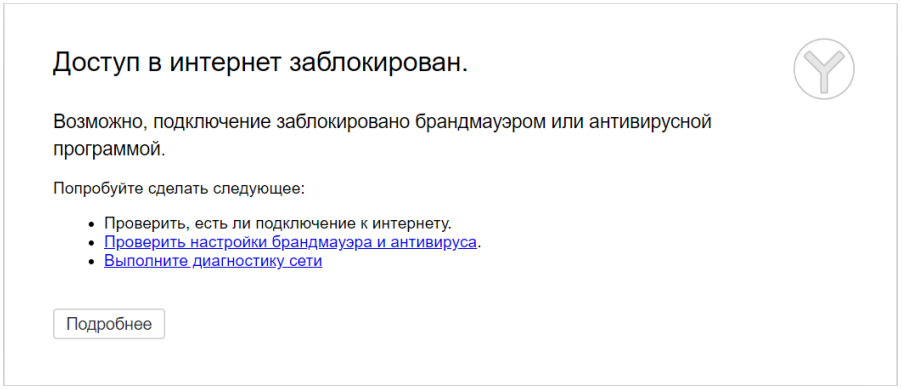
2. *Запрет на подключение с ip-адреса вашего хоста*

Брандмауэр Защитника Windows - Дополнительные параметры - Правила для исходящих подключений - Создать правило



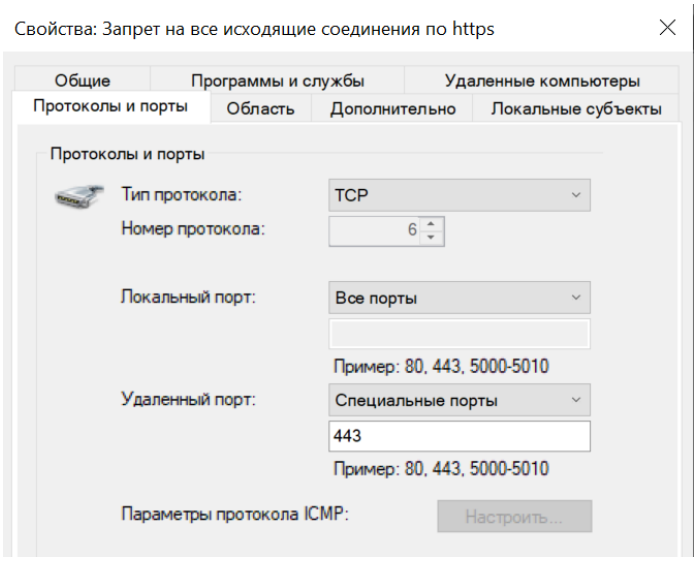
Тип правила: Для порта;
Протокол: TCP;
Определенный локальный порт: все удаленные порты;
Действие: Блокировать подключение.

Результат действия правила:



3. *Запрет на все исходящие соединения по https*
   Брандмауэр Защитника Windows - Дополнительные параметры - Правила для исходящих подключений - Создать правило

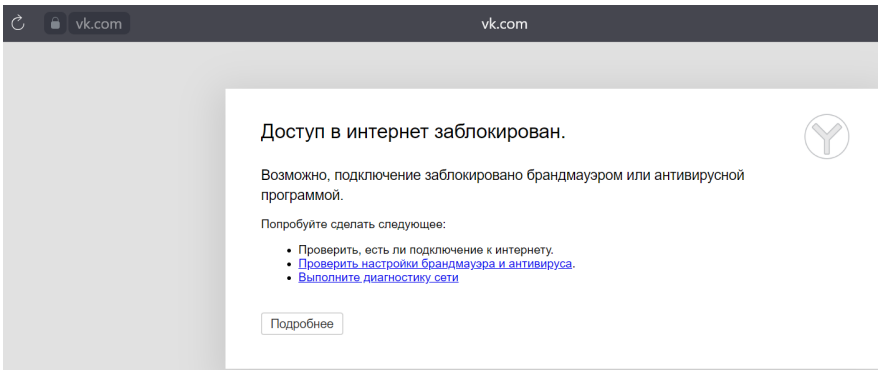
   Тип правила: Для порта;
   Протокол: TCP;
   Определенный локальный порт: 443(https);
   Действие: Блокировать подключение.



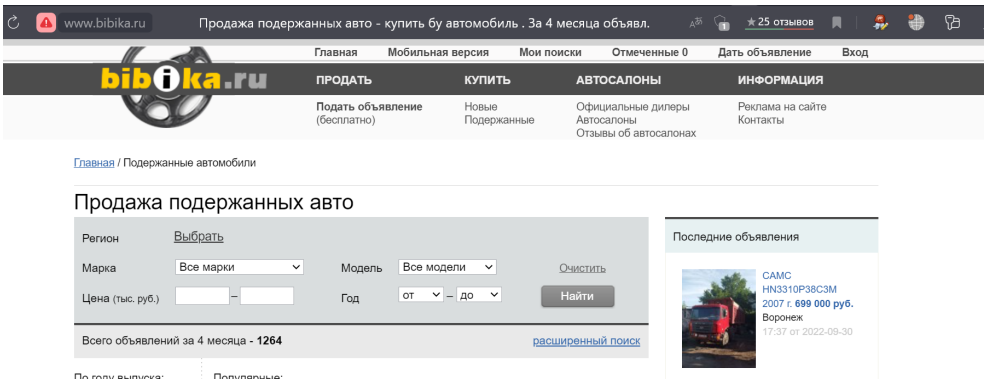
   Результат работы правила: сайты с https заблокированы, http - открываются в штатном режиме.

// список сайтов, работающих по http можно найти, например, следующим запросом в google: “авто -inurl:https”

https://vk.com/



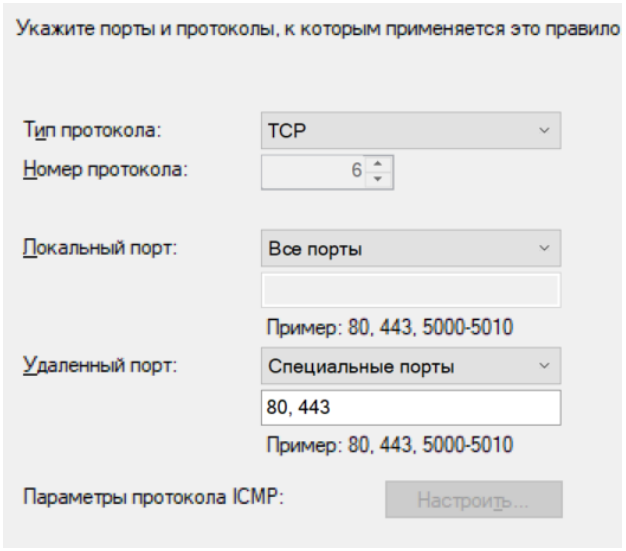
http://www.bibika.ru/catalog/

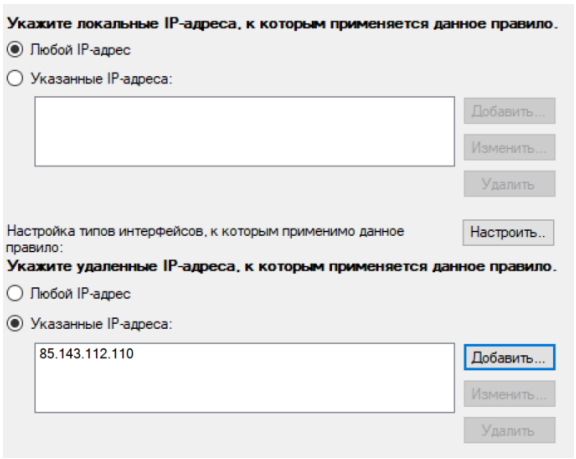


4. *Запретите заходить с виртуальной машины ТОЛЬКО на сайт mephi.ru*
   Брандмауэр Защитника Windows - Дополнительные параметры - Правила для исходящих подключений - Создать правило

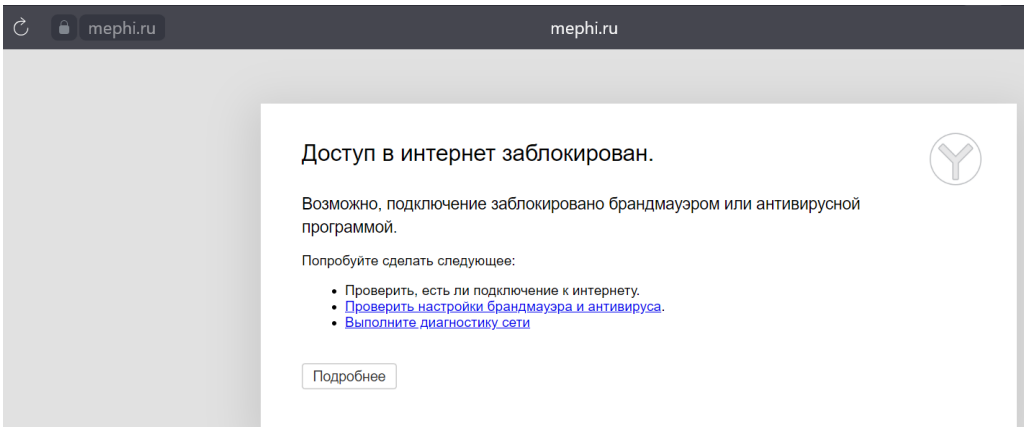
   Тип правила: настраиваемое;
   Программа: все программы;
   Тип протокола: TCP;
   Порты: 80(http), 443(https);

Удаленные ip-адреса, к которым применяется правило: 85.143.112.110 (mephi.ru);
Действие: блокировать подключение.





Правило отрабатывает верно - закрыт доступ только на сайт mephi.ru:



Заключение

В работе были рассмотрены утилиты для настройки межсетевых экранов Linux - firewalld и iptables. Инструменты решают одни и те же задачи, но имеют отличия:

1. firewalld может динамически менять правила обработки трафика, в то время как для iptables необходим перезапуск сервиса;
2. firewalld управляет трафиком на основе зон (наборов правил), iptables - на основе цепочек правил (INPUT, OUTPUT, FORWARD);

firewalld не является межсетевым экраном, а реализован через сетевой фильтр ядра, как и iptables.

Утилиты предоставляют возможность разрешать/блокировать трафик, поступающий/исходящий на машину по разным протоколам, на разные порты, настраивать черные и белые списки и тд.

Изучена работа Windows Firewall на примере создания правил для входящего и исходящего соединения по портам и ip-адресам.